Social Engineering and Technical Security Fusion

Wassim Alexan , *SMIEEE*,
Eyad Mamdouh
Mohamed ElBeltagy
Faculty of IET
The German University in Cairo
Cairo, Egypt
wassim.alexan@ieee.org
eyad.ayad@student.guc.edu.eg
mohamed.elbeltagy@ieee.org

Ahmed Ashraf
Faculty of MET
The German University in Cairo
Cairo, Egypt
ahmedashraf@ieee.org

Mohamed Moustafa,
Hashem Al-Qurashi
Faculty of Informatics and Computer Science
The German International University in Cairo
Cairo, Egypt
mohamed.dawood@student.giu-uni.de
hashem_alqurashi@ieee.org

2022 International Telecommunications Conference (ITC-Egypt) | 978-1-6654-8808-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ITC-Egypt55520.2022.9855761

***Abstract*—Ensuring the secure transmission of sensitive messages over unsecured networks has been a staggering problem in the face of scientists and engineers in recent times. This is exaggerated by developments in cryptanalysis, steganalysis and computing powers at the disposal of hackers. In this paper, a message security scheme that is based on social engineering and technical security fusion is proposed. The proposed scheme makes use of traditional cryptographic algorithms and LSB steganography in addition to ideas pooling from the ever advancing field of social engineering. The provided discussion and numerical analysis showcase the ability of the proposed scheme to fend off cyber attacks.**

***Keywords*–Social engineering, cryptography, steganography, image encryption.**

I.I NTRODUCTION

The speed of development of 5G technology, multimedia and social communication is at a constant rise [1]–[4]. This translates into a monthly global data traffic on the order of exabytes [5]. The implications of such huge data traffic are two–fold. First, comes the issue of security [6], and second all the related transcoding and compression technologies needed [7]. In terms of securing the transmission of sensitive data, 2 large classes of technologies are in use. The first is cryptography, which involves changing the sensitive data into an unrecognizable form through the employment of symmetric and asymmetric algorithms, as well as hash functions to protect it [8]–[10]. Recent literature also introduces the utilization of chaos theory [11], DNA coding [12], cellular automata [13] and many other concepts derived from various fields, for the purposes of multimedia encryption. The second class of technologies is related to information concealment, through steganography or watermarking [14]. This class aims at hiding the sensitive data inside a cover object. This could range from a 2D image [15], [16], a 3D object [17], [18], an audio file [19], a video file [20], or an information matrix [21].

However, not all security threats are of a technical nature. The field of psychology reveals that social engineering (SE) could be just as effective a tool to capsize any of the aforementioned approaches to multimedia security. More specifically, SE is a collection of techniques employed to manipulate victims into releasing sensitive information or taking actions that would compromise data security [22]. In effect, SE works through the exploitation of human weaknesses. This is carried out with various techniques such as phishing, scareware and pretexting [23]. In response, scientists and engineers are developing web applications, software, and advanced filters to mitigate such attacks even before they reach a potential victim's email inbox. Furthermore, for those instances where a malicious email passes through the firewalls, the only standing defensive tool is awareness training [24]. The importance of awareness training is also apparent when realizing that social engineering need not only happen through email messages, but also via phone calls, where firewalls and their like are not even an option [25].

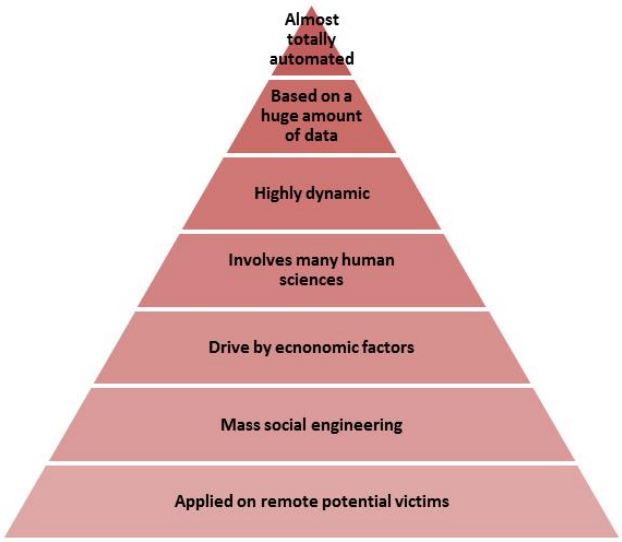

Fig. 1: Features of SE 2.0 (adapted from [26]).

Recent years have witnessed the evolution of SE into Social Engineering 2.0 (SE 2.0), where the aforementioned attacks are utilized in correspondence with naive users' behavior on online social media platforms. This includes the employment of malware ecosystems 2.0, Modern Open Source Intelligence (OSINT), as well as the abuse of psychology, cognitive science models and personality

978-1-6654-8808-2/22/$31.00 ©2022 IEEE

profiling systems [26]. As a matter of fact, recent literature is laden with articles proposing frameworks on SE 2.0 [27], attack models [28] and countermeasures that can be adopted [29]. Fig. 1 illustrates the various features of SE 2.0 with the base of the pyramid starting with attacks that target remote victims, while its top depicts reliance on big data and the utilization of totally automated attacks.

The contributions of this paper are as follows. We propose a secure message transmission scheme over unsecured communication channels, i.e. the Internet. The proposed scheme is based on 2 axes: a technical axis and a non-technical one. The technical axis makes use of a symmetric cipher, AES-256, a hashing protocol, SHA-3 and least significant bit (LSB) steganography in a 2D cover image. The non-technical axis capitalizes on utilizing ideas pooling from the features of SE 2.0, by attempting to "hack the hacker". This combination of security ideas is novel and promises to fend off cyber attacks on sensitive data. This paper is organized as follows. Section II describes the proposed sensitive data security scheme in detail. Section III provides a discussion on the security features of the proposed scheme. Section IV presents the results of the numerical analysis and performance evaluation. Finally, Section V draws the conclusions of the paper and suggests some future research directions.

II. The Proposed Social Engineering and Technical Security Fusion Scheme

At the transmitter side, the proposed security scheme is implemented in the following steps:

1) The sensitive message is hashed, employing SHA3-512.
2) The hashed data is encrypted with a private key, PR_a, employing RSA.
3) The hashed and RSA-encrypted data is concatenated with the binary equivalent sensitive plaintext data.
4) The concatenated data is encrypted with a symmetric key, k, employing AES-256.
5) The resulting bitstream is LSB-embedded in a cover image, resulting in the stego image. An example is shown in Fig. 2.
6) The stego image is encrypted with a rather easy-to-decrypt algorithm, for example, the data encryption standard, (DES). This is shown in Fig. 3.
7) The DES-encrypted image is transmitted over the insecure channel.

Fig. 4 displays a flow chart depicting the transmitting side of the proposed social engineering and technical security fusion scheme.

At the recevier side, the proposed security scheme is implemented in the following steps:

1) The DES-encrypted image is decrypted. This results in an image that matches the one shown in Fig. 2 exactly.
2) The LSB-embedded data is extracted from the stego image.
3) The extracted bitstream is converted back into hexadecimal and AES-256-decrypted employing its symmetric key, k.

Fig. 2: Cover image used to deceive potential hackers.

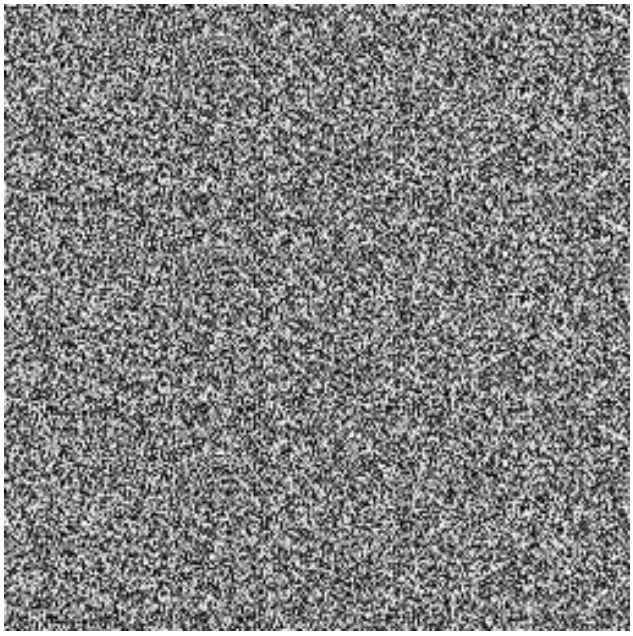

Fig. 3: Encrypted cover image using DES.

4) The data is broken down into 2 strings. The first string is hashed, through usage of SHA3-512, while the second string is RSA-decrypted, utilizing its public key, PU_a.
5) The outputs of the previous step are compared together.

Fig. 5 displays a flow chart depicting the transmitting side of the proposed social engineering and technical security fusion scheme.

III. Discussion of Achieved Security Features

The following subsections discuss the proposed scheme's ability at fending off cyber attacks, both technically (covering the CIA triad) and socially (by utilizing ideas based on SE 2.0).

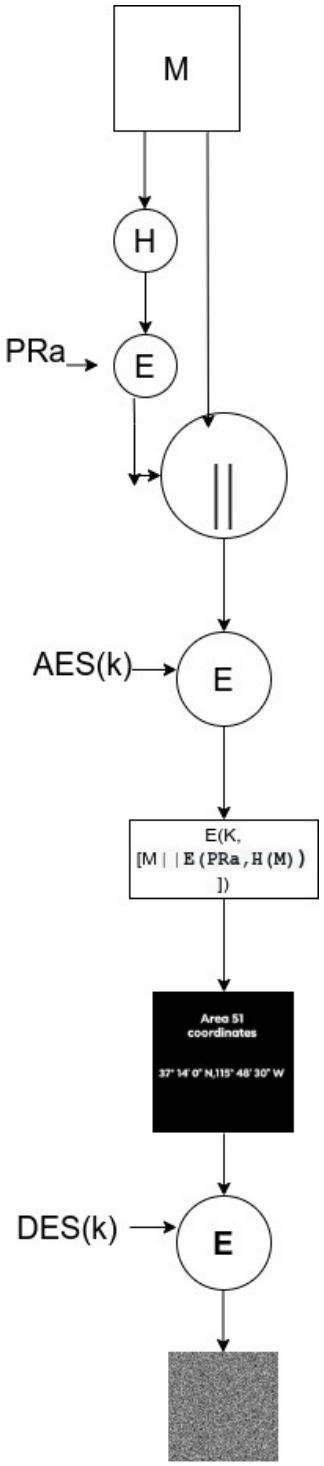

Fig. 4: Flow chart of the proposed social engineering and technical security fusion scheme, at the transmitter side.

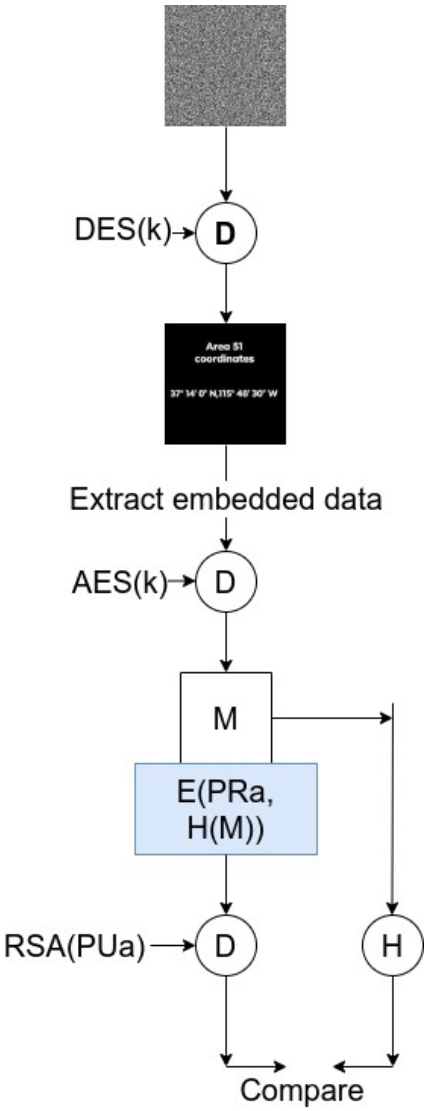

Fig. 5: Flow chart of the proposed social engineering and technical security fusion scheme, at the receiver side.

A. Social Engineering 2.0 Application on Attackers

If an attacker sniffs the network and is able to find the DES-encrypted image, s/he will suppose that the image has sensitive information since it is encrypted. By attempting to decrypt it, s/he will not have a very hard time, since DES is no longer regarded as a very safe encryption algorithm [30]. Upon successfully decrypting the image, the attacker will believe that the image shown in Fig. 2 is itself the actual sensitive message being transmitted over the network. Experiencing emotions of happiness, based on the belief that s/he has successfully gained access to the sensitive information, the attacker will no longer attempt to carry out any further attacks on the image [31]. Thus, the use of this vulnerable security layer of DES image encryption features the utilization of SE 2.0.

B. Confidentiality

Confidentiality is achieved by ensuring that only the legitimate communicating parties have access to the sensitive information. The proposed scheme achieves this through the employment of AES-256 on the contents of the concatenated data and its hashed and encrypted version.

C. User Authentication

User authentication is achieved by the employment of the hashing function SHA3-512 of the message data and encrypting it with the sender's private key. We make use of RSA here to verify user identity via digital signatures [32]. We provide a more elaborate discussion on the combined use of SHA3-512 and RSA to realize user authentication in [33].

D. Integrity

Message integrity (also known as message authentication) is realized in the proposed scheme by means of the hashing function SHA3-512. Employing SHA3-512 ensures that the proposed scheme satisfies both of the one-way property and the collision-free property [33].

IV. Numerical Results and Performance Evaluation

This section outlines the numerical results of the proposed sensitive data transmission scheme. Performance is evaluated in terms of visual and statistical checks and metrics. The proposed scheme is implemented using the computer algebra system Wolfram Mathematica® on a computer running macOS Catalina v10.15.7, with a 2.9 GHz 6-Core Intel® Core™ i9 processor and 32 GB of 2400 MHz DDR4 of memory. Four gray scale images that are commonly used in image processing are utilized in this section. These are Boat, CarAndAPC, Tank and Tank2 (see Fig. 6), as well as the image shown in Fig. 2. All images utilized for testing purposes were of dimensions 256×256.

Table I displays the computed values of a number of well-known evaluation metrics for image processing. A sensitive data string of length 68 characters (544 bits) is utilized. The mean squared errors (MSE) between the cover and stego images are of a small value (~ 0.33), which directly translates into high values of peak signal-to-noise ratio (PSNR) of over 62 dB. With the exception of the Area 51 Coordinates image, entropy values computed for the stego and cover images are identical. For example, $H_C = H_S = 5.54518$ for the Boat image. Moreover, computed SSIM, NCC and image fidelity (IF) values are all very close to 1, indicating a high level of data security provided by the employed steganography layer.

Fig. 7 displays the computation time in seconds for encryption and embedding, extraction and decryption, and finally the total execution time, at various lengths of sensitive data in number of characters, l_m. It is clear that increases in data lengths are proportional with increases in time, however, the relation is not directly proportional. Furthermore, it is noticeable that even for the largest data size ($l_m = 5000$ characters), the total execution time is less than 2.5s, rendering the proposed scheme appropriate for real-time applications on mobile and wireless devices.

V. Conclusions and Future Works

This paper has presented a scheme for secure data transmission that is based on 2 axes, a technical one and a social engineering one. The technical axis made use of a number of technologies, including AES-256, DES, RSA, SHA-512 and LSB steganography. On the other hand, the social engineering axis attempted to make use of a hacker's feelings of success and happiness after correctly decrypting a DES-encrypted image, to fend off any further cryptanalysis efforts on his/her part. A discussion was provided explaining the features provided by the proposed scheme and how they satisfy the CIA triad. Numerical performance evaluation has shown that the proposed scheme presents a combination of cryptography and steganography that is robust against cryptanalysis and steganalysis. Future research efforts could be directed towards the adoption of other useful ideas pooling from SE 2.0.

Fig. 6: Test images utilized. Clockwise from top-left: Boat, CarAndAPC, Tank2 and Tank.

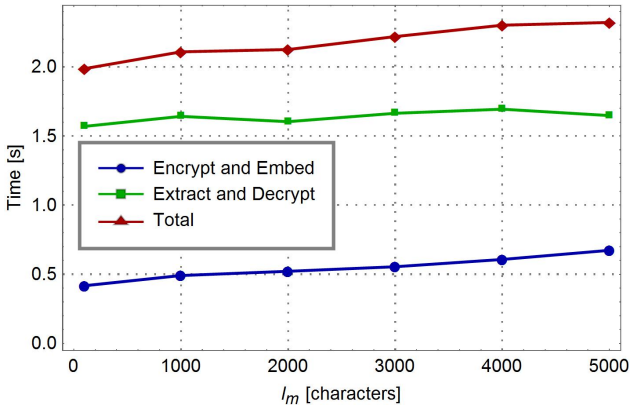

Fig. 7: Execution time at various lengths of sensitive data.

References

[1] A. El Mahdy and W. Alexan, "A threshold-free llr-based scheme to minimize the ber for decode-and-forward relaying," *Wireless Personal Communications*, vol. 100, no. 3, pp. 787–801, 2018.

[2] Y. Sun, T. Wei, H. Li, Y. Zhang, and W. Wu, "Energy-efficient multimedia task assignment and computing offloading for mobile edge computing networks," *IEEE Access*, vol. 8, pp. 36 702–36 713, 2020.

[3] W.-E. Chen and C. H. Liu, "Performance enhancement of virtualized media gateway with dpdk for 5g multimedia communications," in *2019 International Conference on Intelligent Computing and its Emerging Applications (ICEA)*, 2019, pp. 156–161.

[4] C. M. Lentisco, L. Bellido, A. Cárdenas, R. Flores Moyano, and D. Fernández, "Design of a 5g multimedia broadcast application function supporting adaptive error recovery," *IEEE Transactions on Multimedia*, pp. 1–1, 2021.

[5] L. Williams, B. K. Sovacool, and T. J. Foxon, "The energy use implications of 5g: Reviewing whole network operational energy, embodied energy, and indirect effects," *Renewable and Sustainable Energy Reviews*, vol. 157, p. 112033, 2022.

TABLE I: Statistical performance evaluation metrics for a sensitive data string of length 68 characters (544 bits) and gray-scale images of dimensions 256×256.

Image	MSE	PSNR [dB]	H_C	H_S	SSIM	NCC	IF
Area 51 Coordinates	0.0320587	63.0713	1.79694	2.23037	0.998206	1	0.999987
Boat	0.0338287	62.8379	5.54518	5.54518	0.99993	0.999976	0.999994
CarAndAPC	0.337372	62.8497	5.54518	5.54518	0.999863	0.99998	0.999997
Tank	0.0331879	62.921	5.54518	5.54518	0.999771	0.999994	0.999998
Tank2	0.033905	62.8282	5.54518	5.54518	0.999773	0.999983	0.999998

[6] D. A. Shehab and M. J. Alhaddad, "Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research," *Symmetry*, vol. 14, no. 1, p. 117, 2022.

[7] J. Ren, G. Yu, Y. Cai, and Y. He, "Latency optimization for resource allocation in mobile-edge computation offloading," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5506–5519, 2018.

[8] W. Alexan, A. Ashraf, E. Mamdouh, S. Mohamed, and M. Moustafa, "Iomt security: Sha3-512, aes-256, rsa and lsb steganography," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 2021, pp. 177–181.

[9] N. E. El-Meligy, T. O. Diab, A. S. Mohra, A. Y. Hassan, and W. I. El-Sobky, "A novel dynamic mathematical model applied in hash function based on dna algorithm and chaotic maps," *Mathematics*, vol. 10, no. 8, p. 1333, 2022.

[10] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications*, pp. 1–22, 2022.

[11] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Image encryption through lucas sequence, s-box and chaos theory," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 2021, pp. 77–83.

[12] M. Zhang and W. Wu, "Research on image encryption technology based on hyperchaotic system and dna encoding," in *2021 IEEE International Conference on Artificial Intelligence and Industrial Design (AIID)*, 2021, pp. 140–144.

[13] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Lightweight image encryption: Cellular automata and the lorenz system," in *2021 International Conference on Microelectronics (ICM)*, 2021, pp. 34–39.

[14] S. Farrag and W. Alexan, "Secure 3d data hiding technique based on a mesh traversal algorithm," *Multimedia Tools and Applications*, vol. 79, no. 39, pp. 29 289–29 303, 2020.

[15] W. Alexan, A. Elkhateeb, E. Mamdouh, F. Al-Seba'Ey, Z. Amr, and H. Khalil, "Utilization of corner filters, aes and lsb steganography for secure message transmission," in *2021 International Conference on Microelectronics (ICM)*, 2021, pp. 29–33.

[16] W. Alexan and F. Hemeida, "Security through blowfish and lsb bit–cycling with mathematical sequences," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*. IEEE, 2019, pp. 229–234.

[17] A. Samir, W. Alexan, R. T. ElDin, and A. El-Rafei, "3d steganography by random shuffling of image contents using residue model," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2020, pp. 912–918.

[18] Y. Moussa and W. Alexan, "Message security through aes and lsb embedding in edge detected pixels of 3d images," in *2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*. IEEE, 2020, pp. 224–229.

[19] F. Hemeida, W. Alexan, and S. Mamdouh, "A comparative study of audio steganography schemes," *International Journal of Computing and Digital Systems*, vol. 10, pp. 555–562, 2021.

[20] M. Baziyad, T. Rabie, and I. Kamel, "Directional pixogram: A new approach for video steganography," in *2020 Advances in Science and Engineering Technology International Conferences (ASET)*, 2020, pp. 1–5.

[21] M. Mashaly, A. El Saied, W. Alexan, and A. S. Khalifa, "A multiple layer security scheme utilizing information matrices," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*. IEEE, 2019, pp. 284–289.

[22] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003.

[23] S. Gupta, A. Bhattacharya, H. Gupta *et al.*, "Analysis of social engineering attack on cryptographic algorithm," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, 2021, pp. 1–5.

[24] M. Higashino, T. Kawato, M. Ohmori, and T. Kawamura, "An anti-phishing training system for security awareness and education considering prevention of information leakage," in *2019 5th International Conference on Information Management (ICIM)*, 2019, pp. 82–86.

[25] A. Derakhshan, I. G. Harris, and M. Behzadi, "Detecting telephone-based social engineering attacks using scam signatures," in *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics*, ser. IWSPA '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 67–73. [Online]. Available: https://doi.org/10.1145/3445970.3451152

[26] D. Ariu, E. Frumento, and G. Fumera, "Social engineering 2.0: A foundational work," in *Proceedings of the Computing Frontiers Conference*, 2017, pp. 319–325.

[27] K. Zheng, T. Wu, X. Wang, B. Wu, and C. Wu, "A session and dialogue-based social engineering framework," *IEEE Access*, vol. 7, pp. 67 781–67 794, 2019.

[28] A. Suleimanov, M. Abramov, and A. Tulupyev, "Modelling of the social engineering attacks based on social graph of employees communications analysis," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 801–805.

[29] Y. Kano and T. Nakajima, "Trust factors of social engineering attacks on social networking services," in *2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech)*, 2021, pp. 25–28.

[30] B. Shahid, H. Tauqeer, and M. S. Ilyas, "Hardware implementation of des encryption cracker," in *2005 Student Conference on Engineering Sciences and Technology*, 2005, pp. 1–4.

[31] C. Hadnagy, "Social engineering: The science of human hacking. wiley publ," 2018.

[32] P. Kumar and S. K. Sharma, "An empirical evaluation of various digital signature scheme in wireless sensor network," *IETE Technical Review*, pp. 1–11, 2021.

[33] W. Alexan, A. Ashraf, E. Mamdouh, S. Mohamed, and M. Moustafa, "Iomt security: Sha3-512, aes-256, rsa and lsb steganography," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 2021, pp. 177–181.